

Configuration.zipファイルを使用したFMTからFMCへのFDMの移行

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[考慮事項](#)

[コンフィギュレーション](#)

[API要求 – Postman](#)

[ファイアウォール移行ツール](#)

[FMCの検証](#)

[関連情報](#)

はじめに

このドキュメントでは、FMTを使用してFMCに移行するSecure Firewall Device Manager(FDM)の設定file.zipを生成する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ・ シスコファイアウォール脅威対策(FTD)
- ・ Cisco Firewall Management Center(FMC)
- ・ ファイアウォール移行ツール(FMT)
- ・ Postman APIプラットフォーム

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

FTD7.4.2

FMC 7.4.2

FMT 7.7.0.1

ポストマン11.50.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

- FDMは、さまざまな方法でFMCに移行できます。このドキュメントでは、API要求を使用してコンフィギュレーション.zipファイルを生成し、そのファイルを後でFMTにアップロードしてコンフィギュレーションをFMCに移行するシナリオについて説明します。
- このドキュメントに示す手順ではPostmanを直接使用するため、Postmanをインストールしておくことをお勧めします。使用するPCまたはラップトップは、FDMおよびFMCにアクセスする必要があります。また、FMTがインストールされ、実行されている必要があります。

考慮事項

- このドキュメントでは、FMTでの使用よりも多くの設定.zipファイルの生成に焦点を当てています。
- 構成.zipファイルを使用したFDM移行は、非ライブ移行用であり、宛先FTDがすぐに必要になることはありません。

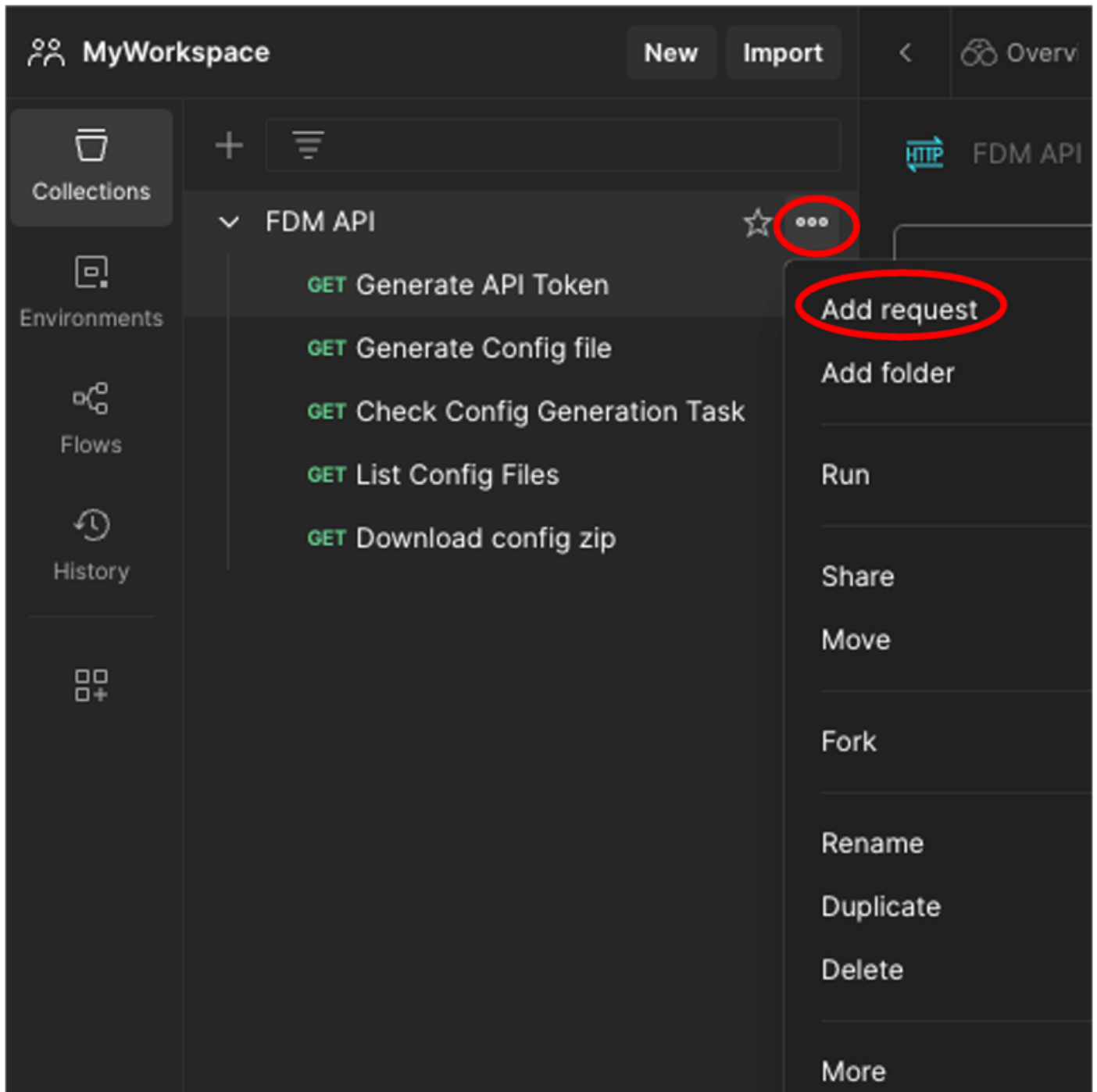


警告：このモードを選択すると、では、アクセスコントロールポリシー(ACP)、ネットワークアドレス変換ポリシー(NAT)、およびオブジェクトのみを移行できます。移行するオブジェクトに関しては、ACPルールまたはNATでそれらのオブジェクトを使用する必要があり、そうでない場合は無視されます。

コンフィギュレーション

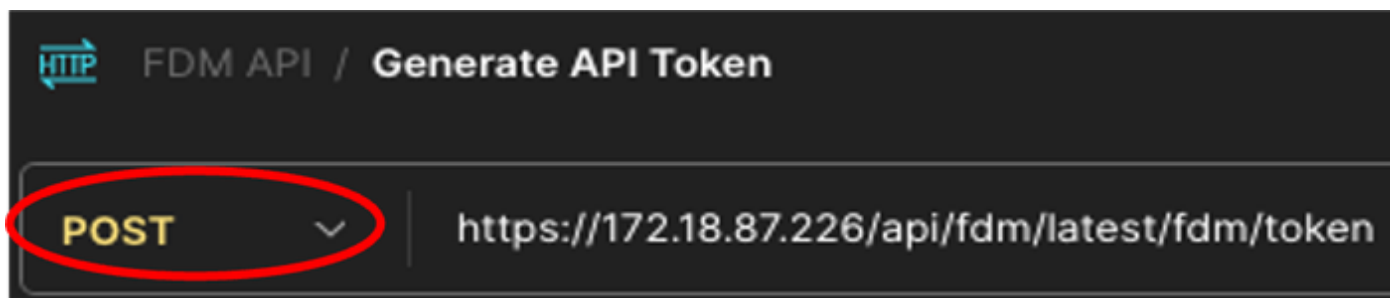
API要求 – Postman

1. Postmanで新しいコレクションを作成します (このシナリオではFDM APIが使用されます)。
2. 3つのドットをクリックし、Add requestをクリックします。



Postman – コレクションの作成と追加の要求

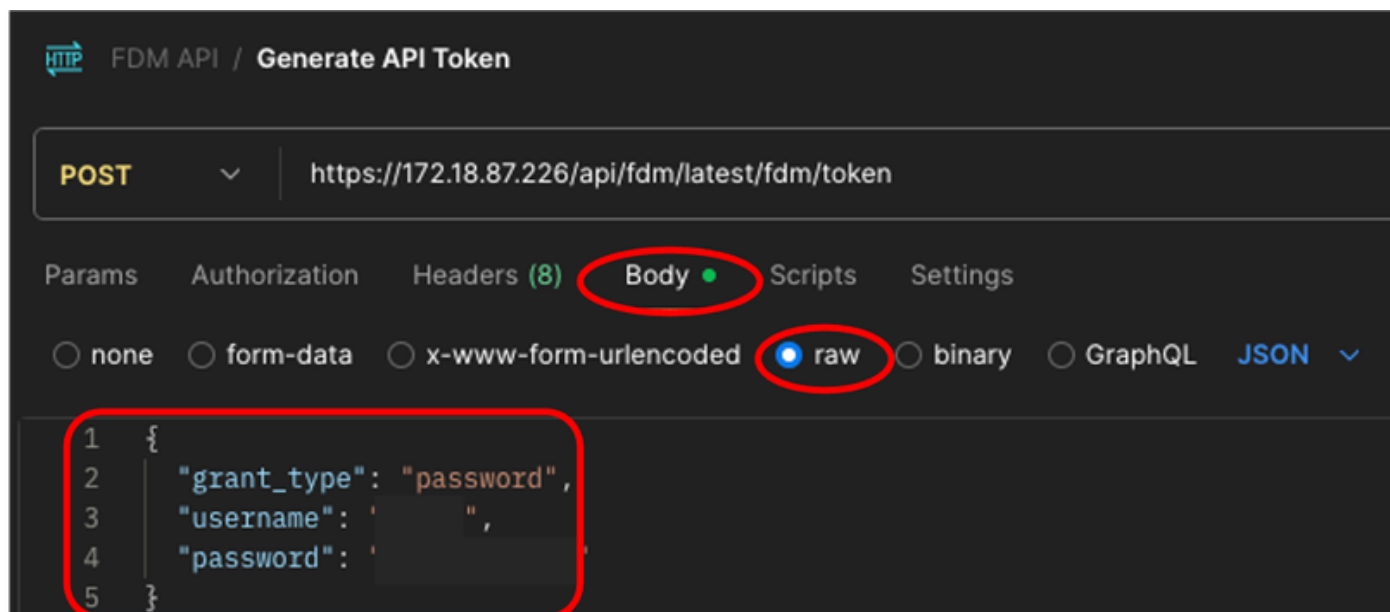
3. この新しい要求を呼び出します： APIトークンを生成します。これはGET要求として作成されますが、この要求を実行するときには、ドロップダウンメニューからPOSTを選択する必要があります。POSTの横のテキストボックスに、次の行https://<FDM IP
ADD>/api/fdm/latest/fdm/tokenを挿入します



Postman : トークン要求

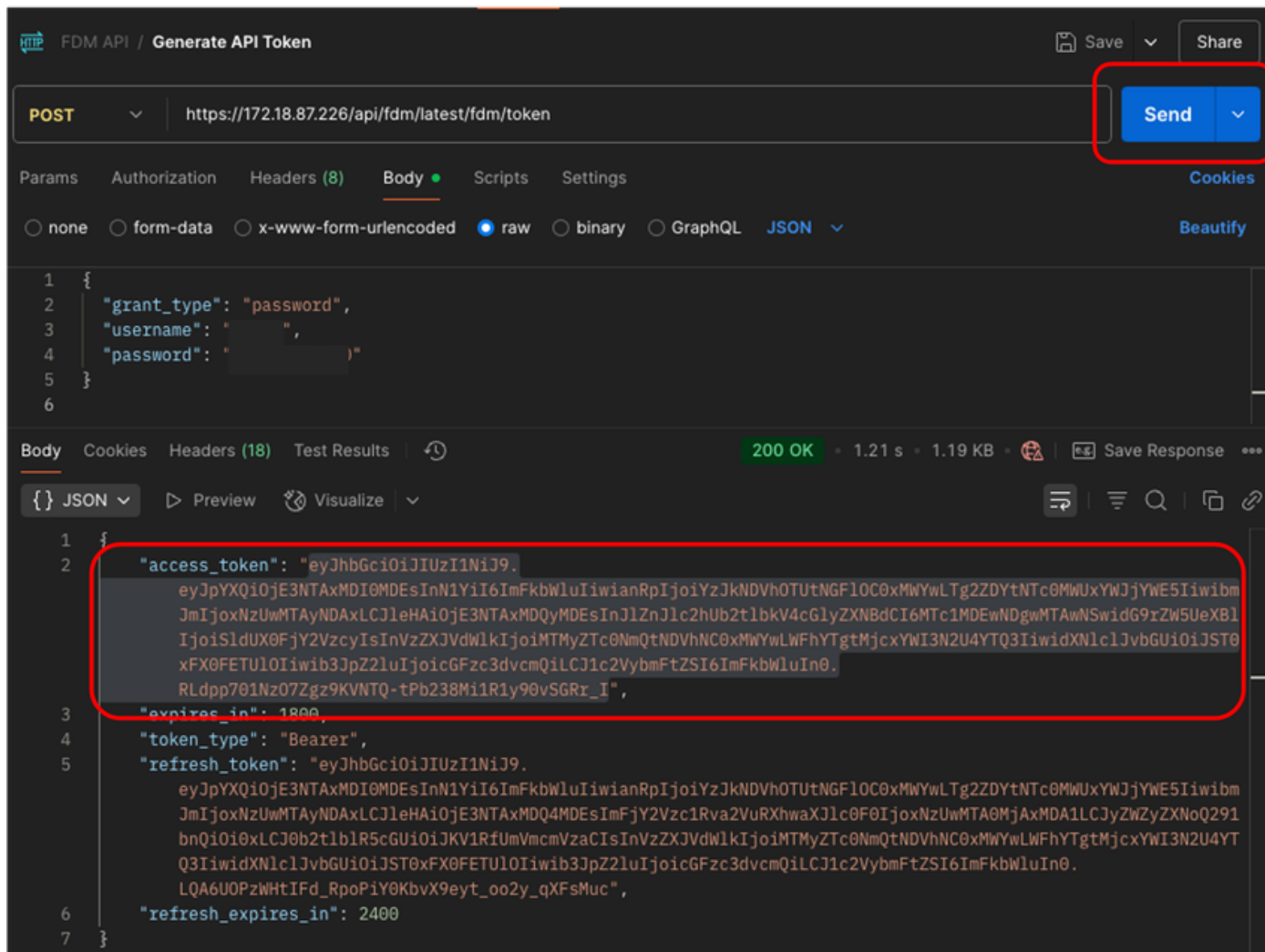
4. 「本体」タブで「raw」オプションを選択し、このフォーマットを使用してFTD(FDM)デバイスにアクセスするための「資格証明」を入力します。

```
{  
  "grant_type": "password",  
  "username": "username",  
  "password": "password"  
}
```



Postman – トークン要求本文

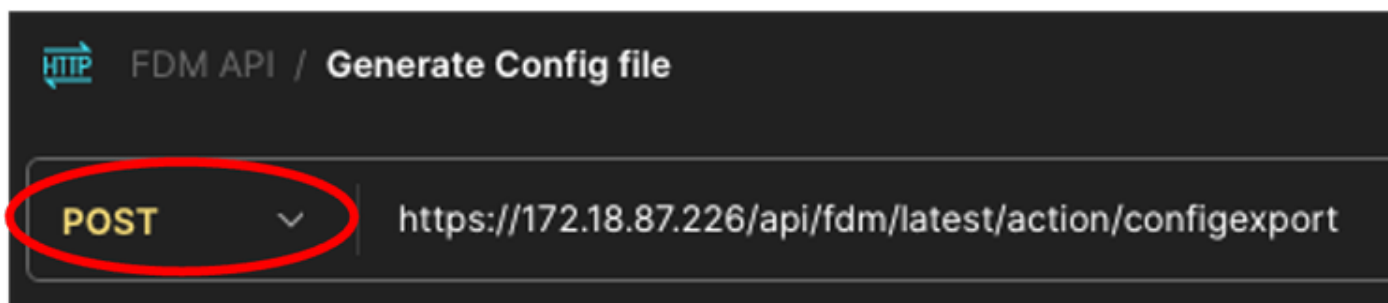
5. 最後に、Sendをクリックしてアクセストークンを取得します。問題がなければ、200 OKの応答を受信します。トークン全体のコピーを作成します (ダブルクォート内)。これは、後の手順で使用します。



Postman – トークンが正常に生成されました

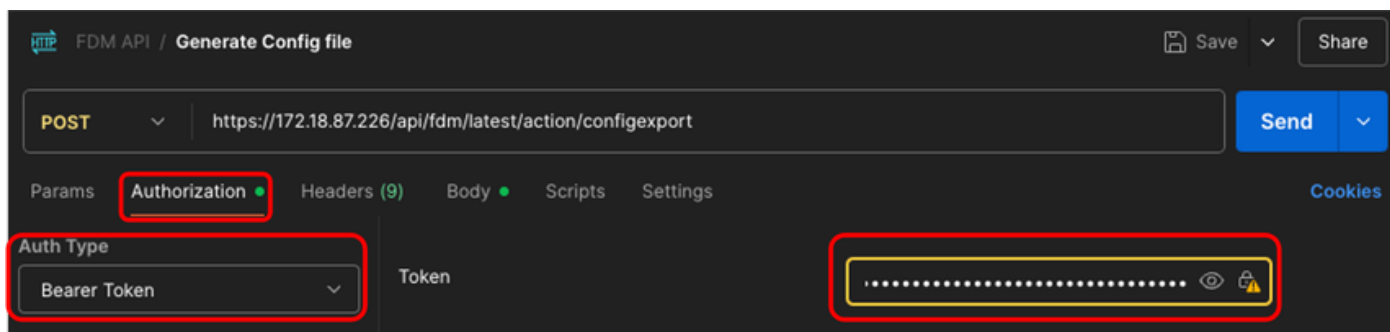
6. ステップ2を繰り返して新しい要求を作成し、POSTを再度使用します。

7. この新しい要求を「構成ファイルの生成」と呼びます。これはGET要求として作成されますが、この要求を実行するときには、ドロップダウンメニューからPOSTを選択する必要があります。POSTの横のテキストボックスに、次の行`https://<FDM IP ADD>/api/fdm/latest/action/configexport`を挿入します



Postman – 構成ファイル要求の生成

8. Authorizationタブで、ドロップダウンメニューからBearer Token as Auth Typeを選択し、Tokenの横のテキストボックスにステップ5でコピーしたトークンを貼り付けます。



Postman – 構成ファイルの生成要求 – 承認

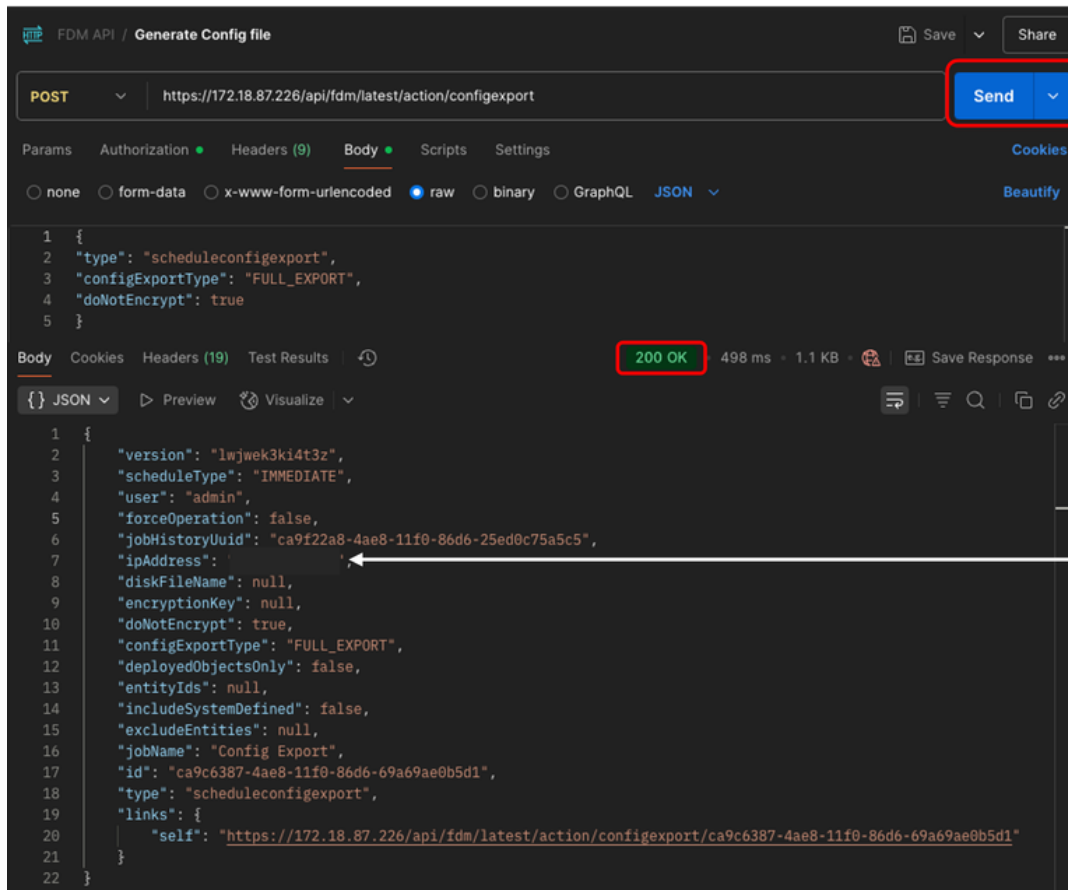
9. 「本体」タブで「raw」オプションを選択し、この情報を入力します。

```
{  
  「タイプ」: 「scheduleconfigexport」、  
  "configExportType": "FULL_EXPORT",  
  "doNotEncrypt": true  
}
```



Postman – 構成ファイル要求の生成 – 本文

10. 最後に、Sendをクリックします。問題がなければ、200 OKの応答を受信します。

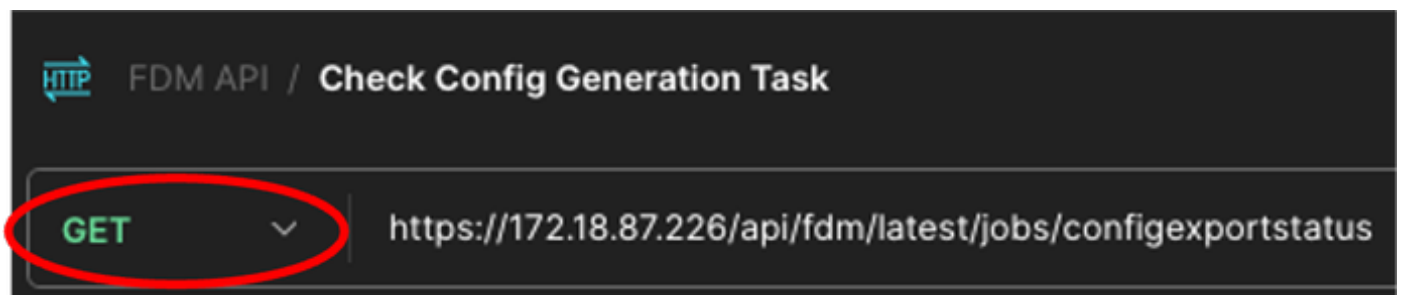


This IP address is the one that is connecting to the FTD through the requests.

Postman – 構成ファイル要求の生成 – 出力

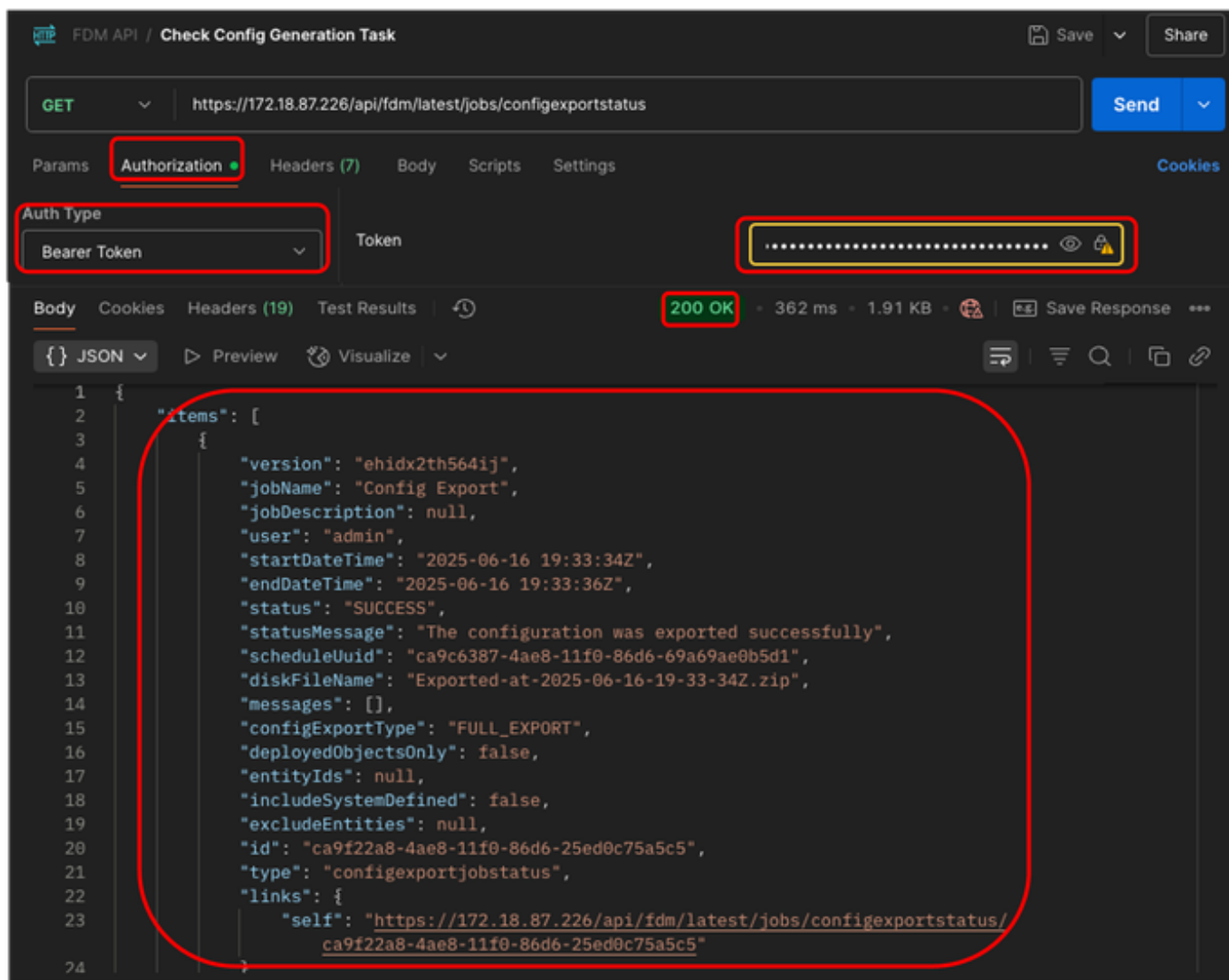
11. ステップ2を繰り返して、新しい要求を作成します。GETは今回は使用します。

12. この新しい要求を「Check Config Generation Task」と呼びます。これはGET要求として作成されます。また、このコマンドを実行するときには、ドロップダウンメニューからGETを選択する必要があります。GETの横のテキストボックスに、次の行https://<FDM IP ADD>/api/fdm/latest/jobs/configexportstatus



Postman : 設定エクスポートステータス要求の確認

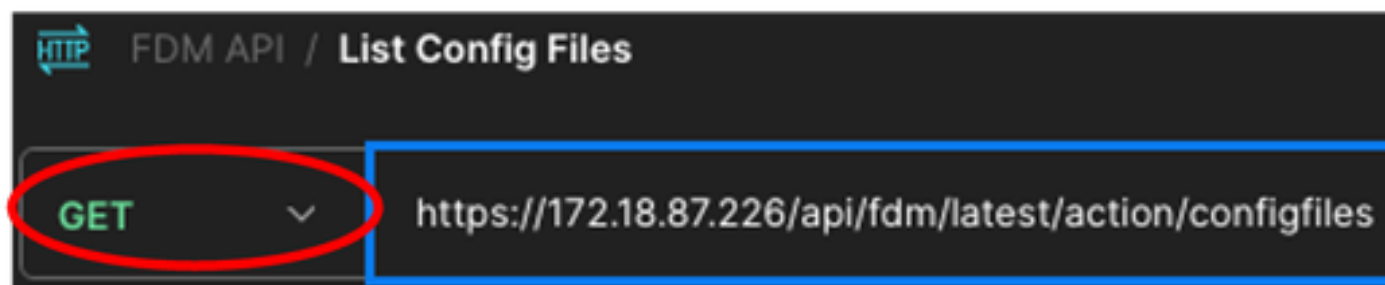
13. Authorizationタブで、ドロップダウンメニューからBearer Token as Auth Typeを選択し、Tokenの横のテキストボックスにステップ5でコピーしたトークンを貼り付けます。最後に、Sendをクリックします。問題がなければ、200 OK応答を受信し、JSONフィールドにタスクのステータスやその他の詳細を表示できます。



Postman:Config Export Status Request : 許可および出力

14. ステップ2を繰り返して新しい要求を作成するため、今回はGETを使用します。

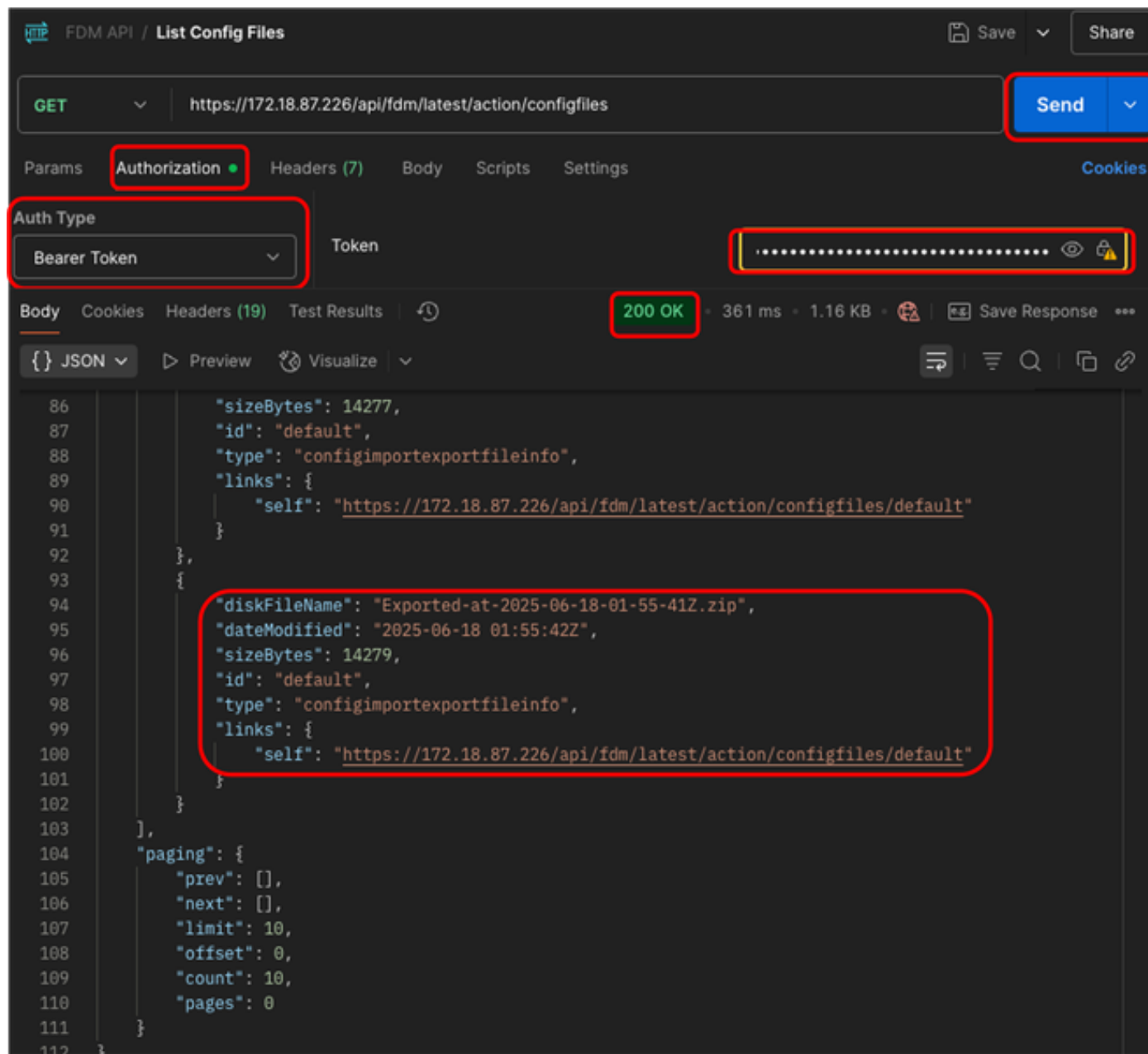
15. この新しい要求を「List Config Files」と呼びます。GET要求はGET要求として作成されますが、この要求を実行する際に、ドロップダウンメニューからGETを選択する必要があります。GETの横のテキストボックスに、次の行`https://<FDM IP ADD>/api/fdm/latest/action/configfiles`を挿入します



Postman - エクスポートされた構成ファイルの一覧表示の要求

16. Authorizationタブで、ドロップダウンメニューからBearer Token as Auth Typeを選択し、Tokenの横のテキストボックスにステップ5でコピーしたトークンを貼り付けます。最後に、

Sendをクリックします。問題がなければ、200 OK応答を受信し、JSONフィールドにエクスポートされたファイルのリストが表示されます。最新のものが下部に表示されます。最新のファイル名（ファイル名のより新しい日付）をコピーします。これは、このファイル名が最後のステップで使用するためです。

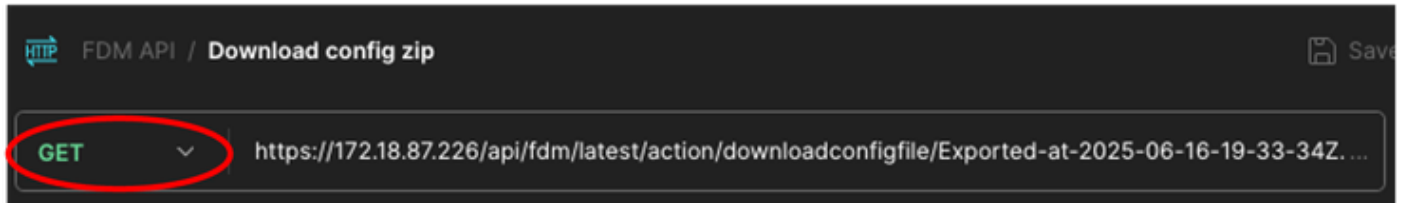


Postman – エクスポートされた設定ファイルの一覧表示リクエスト – 許可と出力

17. ステップ2を繰り返して新しい要求を作成するため、今回はGETを使用します。

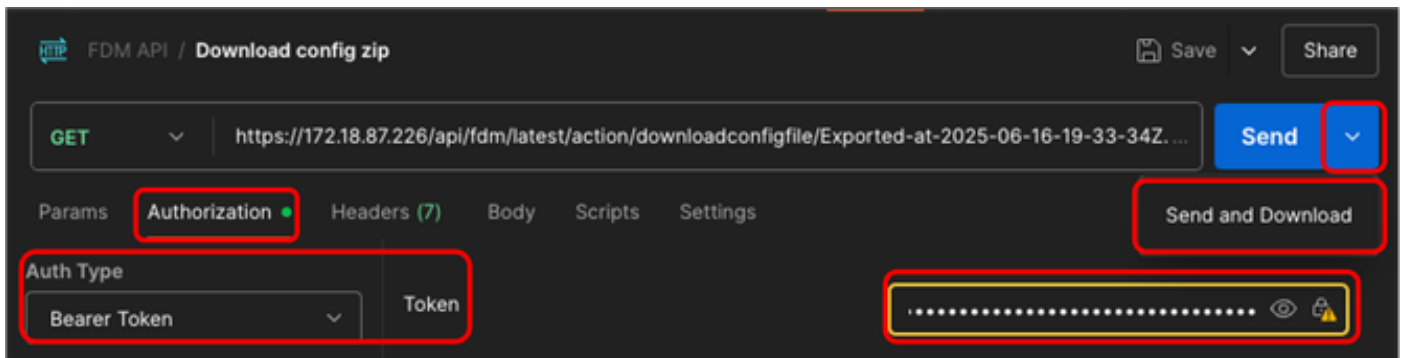
18. 次の新しい要求を呼び出します。config zipをダウンロードします。GET要求はGET要求として作成されますが、この要求を実行する際に、ドロップダウンメニューからGETを選択する必要があります。GETの横のテキストボックスに次の行を挿入し、手順16でコピーしたファイル名を最後に貼り付けます。https://<FDM IP

ADD>/api/fdm/latest/action/downloadconfigfile/<Exported_File_name.zip >



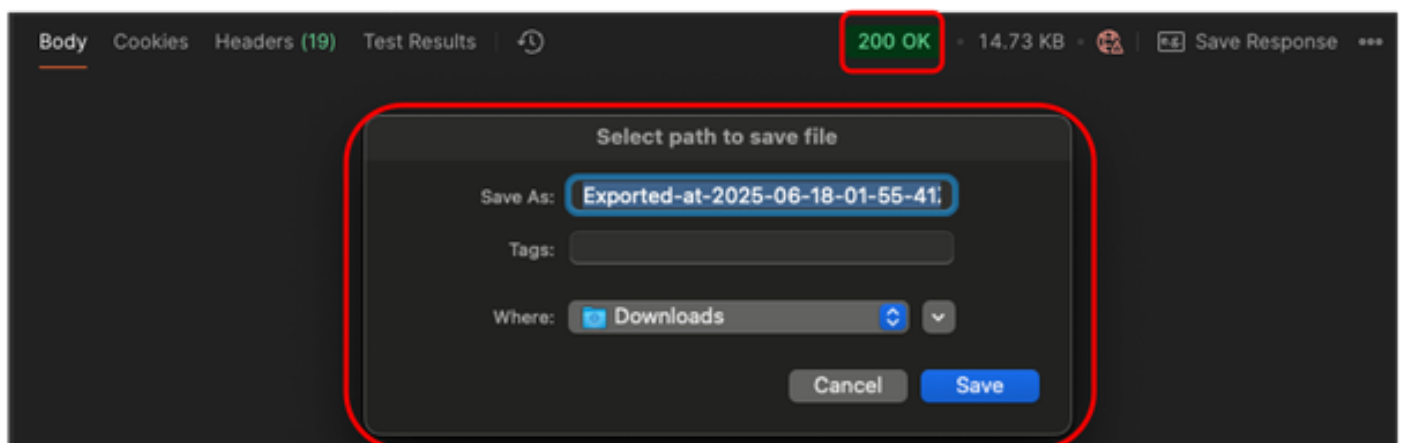
Postman:Config.zipファイル要求のダウンロード

19. Authorizationタブで、ドロップダウンメニューからBearer Token as Auth Typeを選択し、Tokenの横のテキストボックスに、ステップ5でコピーしたトークンを貼り付けます。最後に、Sendの横にある下矢印をクリックして、Send and Downloadを選択します。



Postman - Config.zipファイルのダウンロード要求 - 許可

20. 問題がなければ、200 OK応答が表示され、configuration.zipファイルの保存先フォルダを指定するよう求めるポップアップウィンドウが表示されます。これで、この.zipファイルをファイアウォール移行ツールにアップロードできます。



Postman - Config.zipファイルのダウンロード要求 - 保存

ファイアウォール移行ツール

21. Firewall Migration Toolを開き、Select Source Configurationドロップダウンメニューで、Cisco Secure Firewall Device Manager (7.2+)を選択し、Start Migrationをクリックします。

Firewall Migration Tool (Version 7.7)

Select Source Configuration

Source Firewall Vendor

Cisco Secure Firewall Device Manager (7.2+)

Start Migration Demo Mode

Cisco Secure Firewall Device Manager (7.2+) Pre-Migration Instructions

This migration may take a while. Do not make any changes to the Firewall Management Center (FMC) and Firewall Device Manager (FDM) when migration is in progress. FDM to FMC manager movement process should be done over a downtime/maintenance window. FDM Devices enrolled with the cloud management will lose access upon registration with FMC.

Session Telemetry:
Cisco collects the firewall telemetry set forth below in connection with this migration. By completing the migration, you consent to Cisco's collection and use of this telemetry data for purposes of tracking and following up on firewall device migrations and performing related migration analytics.

Acronyms used:
FMT: Firewall Migration Tool
FTD: Firewall Threat Defense
FMC: Firewall Management Center
FDM: Firewall Device Manager

Before you begin your Firewall Device Manager (FDM) to Firewall Threat Defense migration, you must have the following items:

- **Stable IP Connection:**
Ensure that the connection is stable between FMT, FDM and FMC. The host-pc from which the Firewall Migration tool is being run, should have connectivity to the FDM and the FMC.
- **FMC and FDM Version:** Ensure that the FMC version is 7.3 or later and FDM version is 7.2 or later. FDM version should be always equal or less than the FMC version. For optimal migration time, improved software quality and stability, use the suggested release for your **FTD** and **FMC**. Refer to the gold star on CCO for the suggested release.
- **FMC Requirements:**
Create a dedicated user account with administrative privileges for the FMT and use the credentials during migration. RestAPI is enabled on FMC by default. It is highly recommended that this is checked before migration. FMC should be registered with smart licensing server, and the licenses enabled on FDM must be enabled on FMC for smooth onboarding.
- **FDM Migration Options :**
Migration from FDM is supported in following ways.
 1. **Migrate Firewall Device Manager (Shared Configurations Only)**
 - This option migrates shared configuration to FMC.
 - This approach should be used to stage shared configuration to FMC. Maintenance window is not required.
 - User can either upload a configuration bundle or provide FDM credentials to fetch details.
 - Automated fetching of configuration is a preferred method.
 2. **Migrate Firewall Device Manager (Includes Device & Shared Configurations)**
 - This option migrates both device and shared configuration. Same FTD is moved from FDM managed to FMC managed.
 - **The migration process is to be done over a scheduled downtime or maintenance window. There is device downtime involved in this migration process.**
 - Ensure connectivity between FDM device and FMC to move the device from FDM to FMC using FDM.
 - Ensure FDM Configuration has AD Realm with encryption set to NONE. [Click here](#) for more info.
 - User should provide FDM IP and credentials to fetch details. Uploading configuration bundle is not supported.
 - FDM Devices enrolled with the cloud management will lose access upon registration with FMC.
 - Ensure out-of-band access to FTD device is available, to access the device in case of accessibility issues during migration.
 - It is highly recommended that a backup (export) of the FDM configuration is performed to restore the original state of the firewall managed by FDM if required.
 - If the FTD devices are in a failover pair, failover needs to be disabled (break HA) before proceeding with moving manager from FDM to FMC.
 - FDM with Universal PLR cannot be moved from FDM to FMC.
 - FDM with flexConfig objects or flexconfig policies cannot be moved from FDM to FMC. The flexconfig objects and policies must be

FMT - FDM選択

22. 最初のオプションボタンをチェックし、Migrate Firewall Device Manager (Shared Configurations Only)にチェックマークを入れて、Continueをクリックします。

How would you like to migrate from Firewall Device Manager :



Click on text below to get additional details on each of the migration options

☒ Migrate Firewall Device Manager (Shared Configurations Only)

- This option migrates shared configuration to FMC.
- This approach should be used to stage shared configuration to FMC. Maintenance window is not required.
- User can either upload a configuration bundle or provide FDM credentials to fetch details.
- Automated fetching of configuration is a preferred method.

☐ Migrate Firewall Device Manager (Includes Device & Shared Configurations)

☐ Migrate Firewall Device Manager (Includes Device & Shared Configurations) to FTD Device (New Hardware)

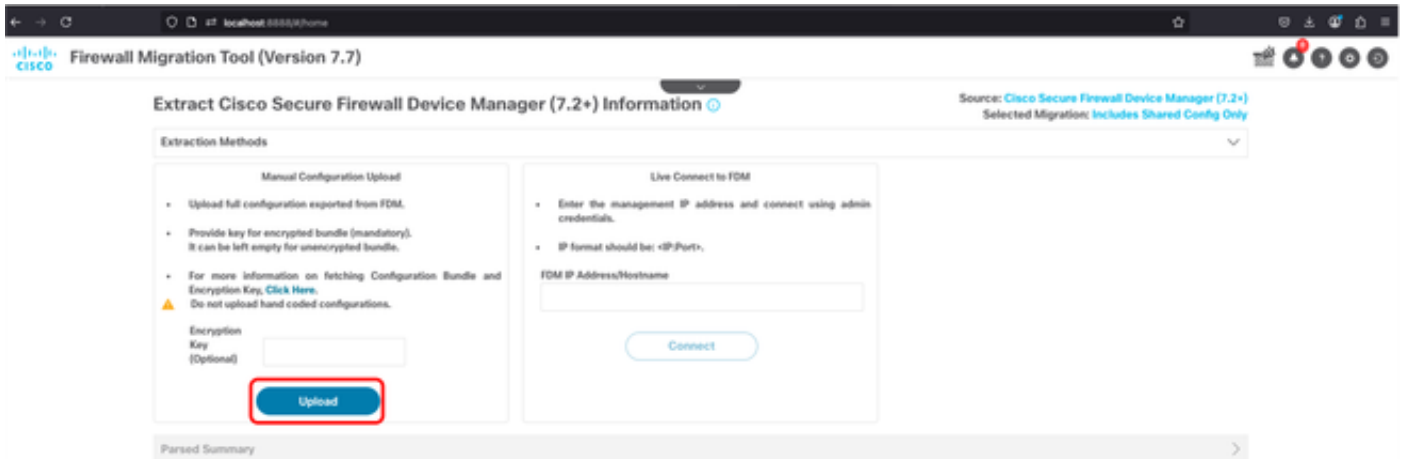
Note :

- Device configuration includes Interfaces, Routes and Site to Site VPN based features.
- Shared configuration includes Access control Policy, Remote Access VPN, NAT and Objects based features.

Continue

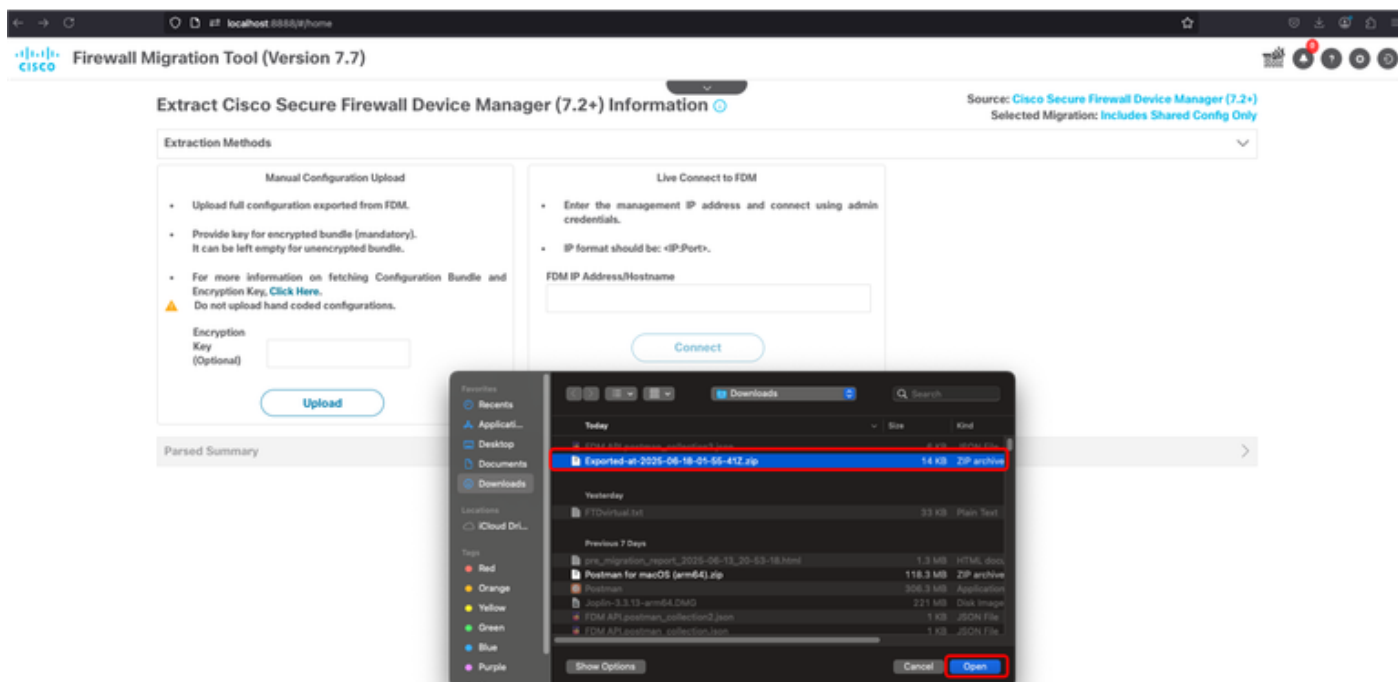
FMT - FDM移行共有構成のみ

23. 左側のパネル(Manual Configuration Upload)でUploadをクリックします。



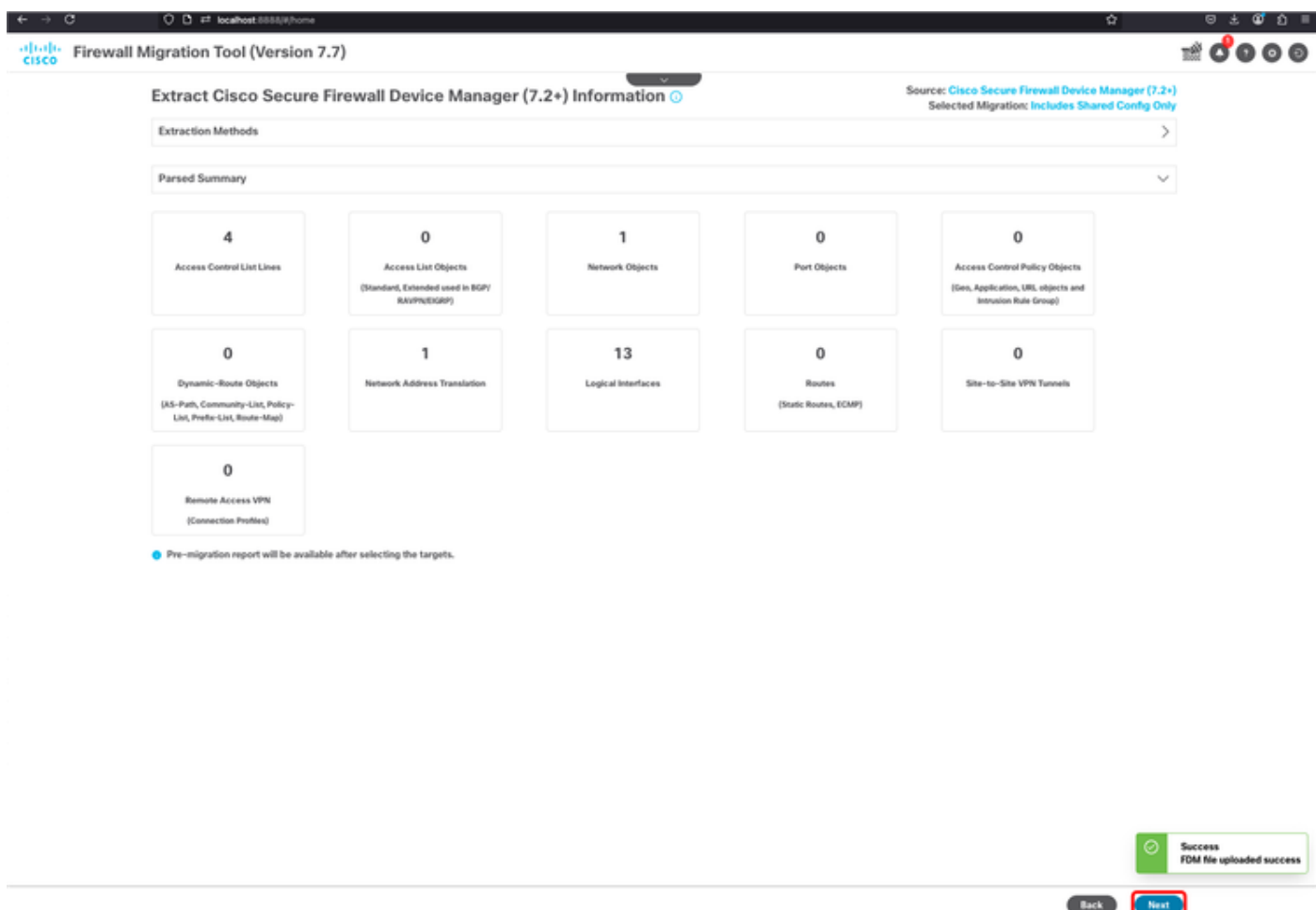
FMT:Config.zipファイルのアップロード

24. 前に保存したフォルダでエクスポートしたzip設定ファイルを選択し、開くをクリックします。



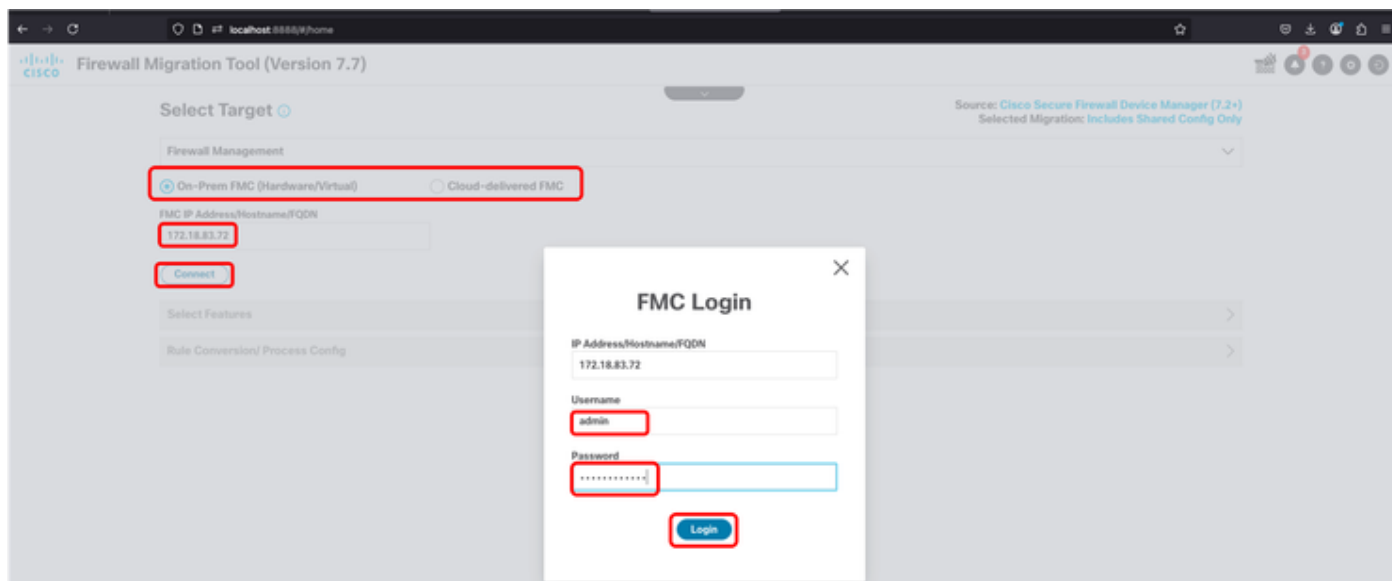
FMT - Config.zipファイルの選択

25. すべてが期待どおりに進んだ場合は、「解析された要約」が表示されます。また、右下隅に、FDMファイルが正常にアップロードされたことを通知するポップアップが表示されます。[Next] をクリックします。



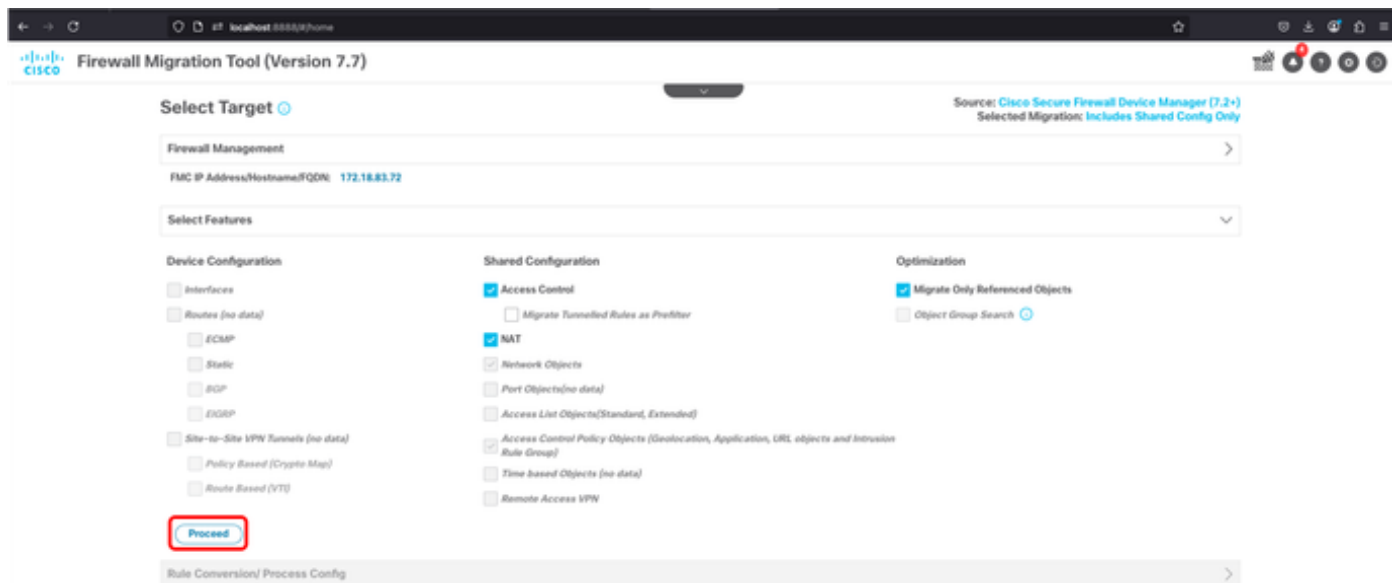
FMT – 解析の概要

26. 環境に適したオプション (オンプレミスFMCまたはCd-FMC) をチェックします。このシナリオでは、オンプレミスFMCが使用されます。FMC IP addressを入力し、Connectをクリックします。新しいポップアップが表示され、FMCクレデンシャルの入力を求められます。この情報を入力したら、Loginをクリックします。



FMT:FMCターゲット・ログイン

27. 次の画面には、移行されるターゲットFMCと機能が表示されます。[続行 (Proceed)] をクリックします。



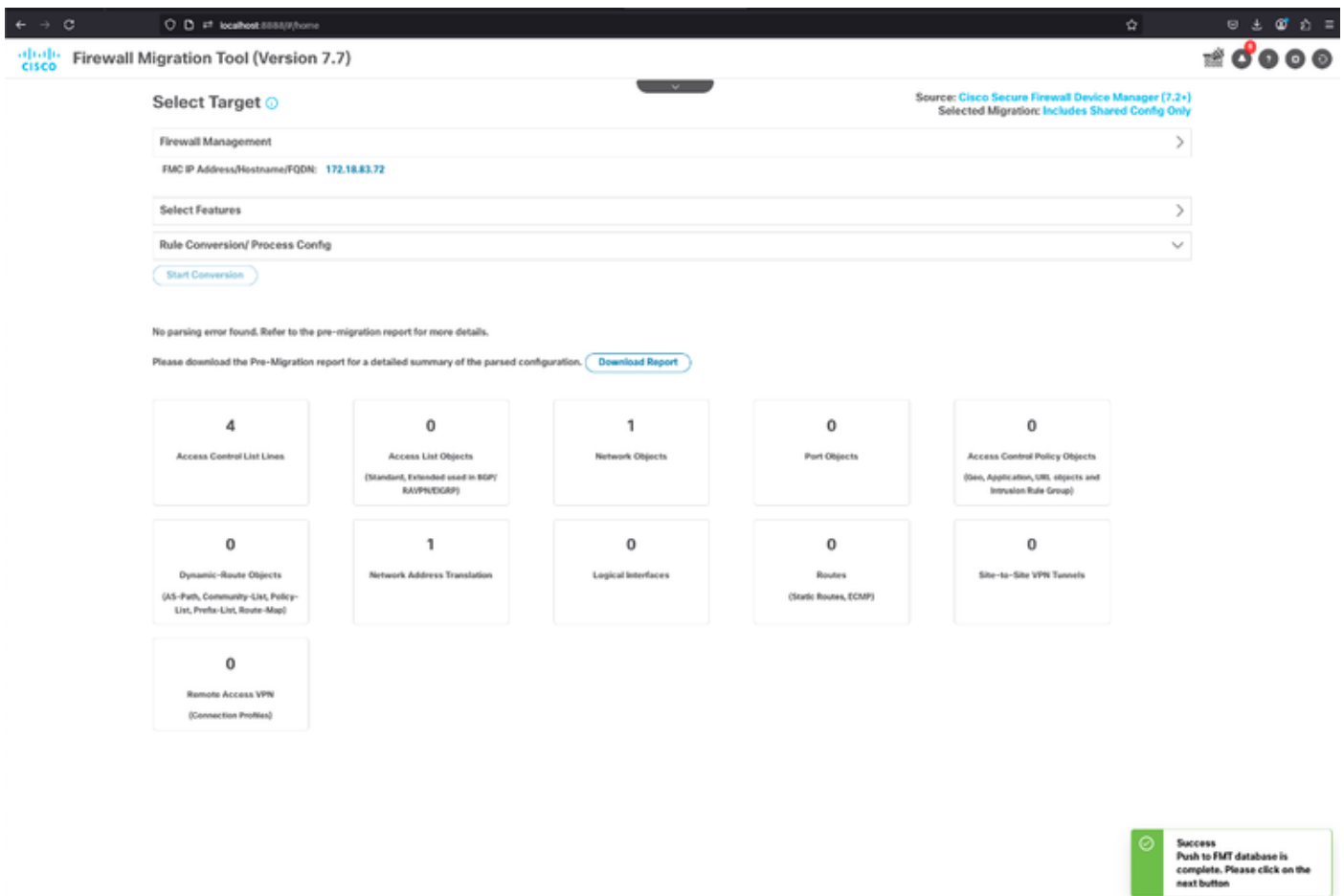
FMT - FMCターゲット - 機能選択

28. FMCターゲットが確定したら、Start Conversionボタンをクリックします。



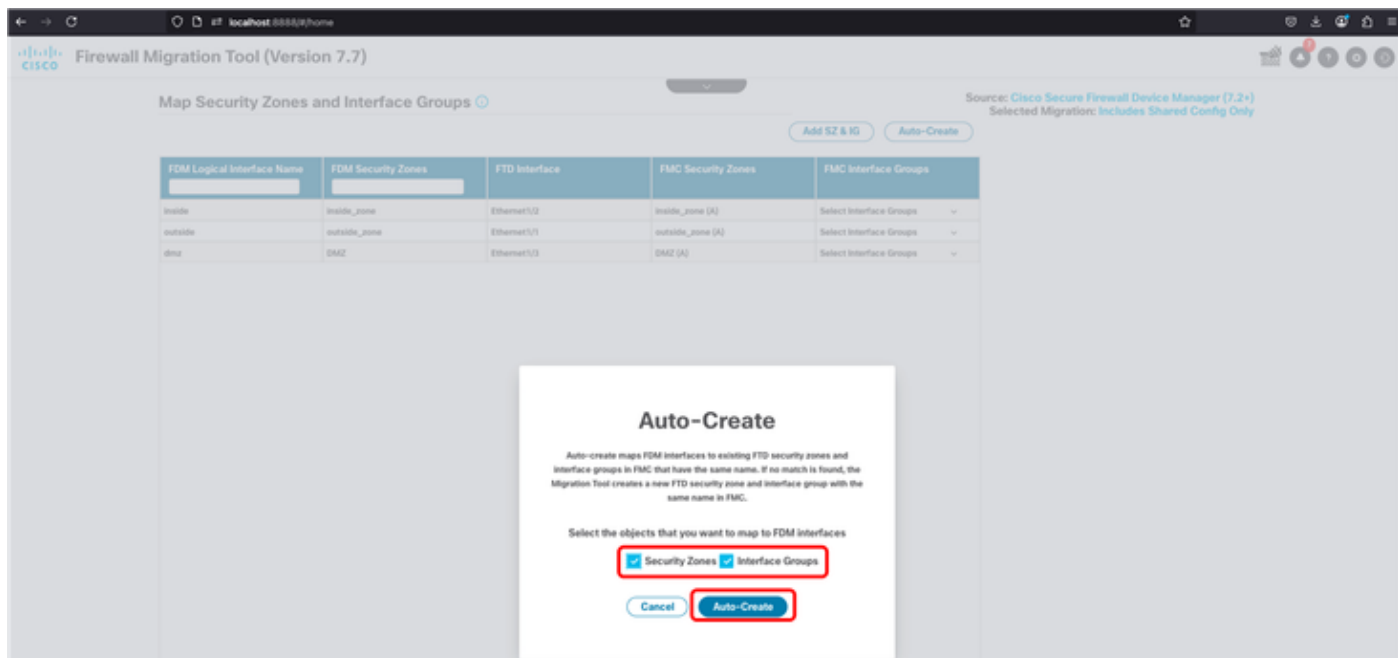
FMT:Config Conversionの開始

29. すべてが正しく行われると、右下にポップアップが表示され、FMTデータベースへのプッシュが完了したことが通知されます。[Next] をクリックします。



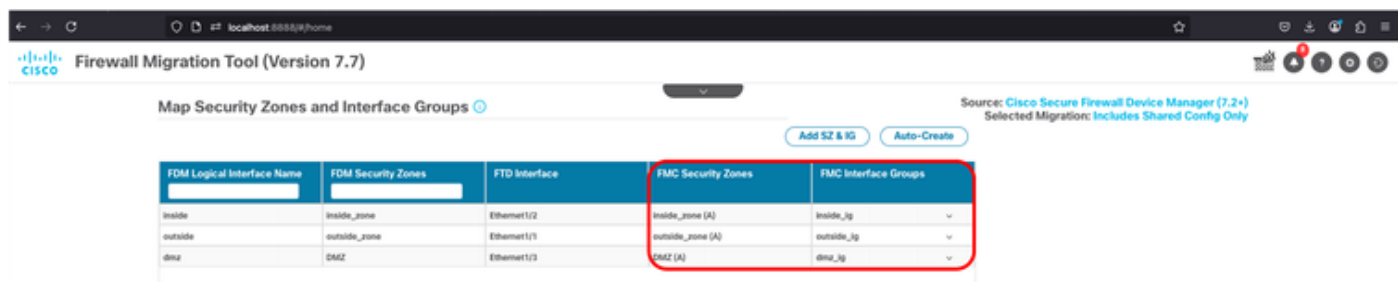
FMT – データベースのプッシュが正常に完了しました

30. 次の画面で、手動で作成するか、またはセキュリティゾーンとインターフェイスグループの自動作成を選択する必要があります。このシナリオでは、auto-createが使用されます。



FMT:Auto Creating Security Zones and Interface Groups (セキュリティゾーンおよびインターフェイスグループの自動作成)

31. 完了すると、表の4列目と5列目に、それぞれセキュリティゾーンとインターフェイスグループが表示されます。



FMT : セキュリティゾーンとインターフェイスグループが正常に作成されました

32. 次の画面では、ACLを最適化するか、ACP、オブジェクト、およびNATを検証できます。完了したら、Validateボタンをクリックします。

Firewall Migration Tool (Version 7.7)

Optimize, Review and Validate Shared Configuration Only

Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Migration: Includes Shared Config Only

Access Control Objects NAT Interfaces Routes Site-to-Site VPN Remote Access VPN

AGP Pre-filter Intrusion Policy

Select all 4 entries Selected: 0 / 4

Search

#	Name	SOURCE			DESTINATION			ACCESS CONTROL POLICY ...		State	Action	ACE Count	TIME BASED
		Zone	Network	Port	Zone	Network	Port	Applications	URLs				
1	Inside_Outside_Rul...	inside_zone	ANY	ANY	outside_in...	ANY	ANY	ANY	ANY	✓	trust	1	None
2	AD-Srvr_R1	DMZ	AD-Srvr	ANY	inside_zone	ANY	ANY	ANY	ANY	✓	permit	1	None
3	DMZ-Inside_R1	DMZ	ANY	ANY	inside_zone	ANY	ANY	ANY	ANY	✓	deny	1	None
4	Outside_DMZ_R1	outside_in...	ANY	ANY	DMZ	ANY	ANY	ANY	ANY	✓	permit	1	None

50 per page 1 to 4 of 4 Page 1 of 1

Optimize ACL Validate

FMT:ACLの最適化：移行の検証

33. 検証が完了するまで数分かかります。

Firewall Migration Tool (Version 7.7)

Optimize, Review and Validate Shared C

Validation in progress. It will take a while

Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Migration: Includes Shared Config Only

Access Control Objects NAT Interfaces Routes Site-to-Site VPN Remote Access VPN

AGP Pre-filter Intrusion Policy

Select all 4 entries Selected: 0 / 4

Search

#	Name	SOURCE			DESTINATION			ACCESS CONTROL POLICY ...		State	Action	ACE Count	TIME BASED
		Zone	Network	Port	Zone	Network	Port	Applications	URLs				
1	Inside_Outside_Rul...	inside_zone	ANY	ANY	outside_in...	ANY	ANY	ANY	ANY	✓	trust	1	None
2	AD-Srvr_R1	DMZ	AD-Srvr	ANY	inside_zone	ANY	ANY	ANY	ANY	✓	permit	1	None
3	DMZ-Inside_R1	DMZ	ANY	ANY	inside_zone	ANY	ANY	ANY	ANY	✓	deny	1	None
4	Outside_DMZ_R1	outside_in...	ANY	ANY	DMZ	ANY	ANY	ANY	ANY	✓	permit	1	None

FMT:Validation in Progress (検証中)

34. 設定が完了すると、FMTによって設定が正常に検証されたことが通知され、次のステップとしてPush Configurationボタンをクリックします。

×

Validation Status

✓

Successfully Validated

Validation Summary (Pre-push)

4 Access Control List Lines	Not selected for migration Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)	1 Network Objects	Not selected for migration Port Objects	0 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)
Not selected for migration Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)	1 Network Address Translation	Not selected for migration Logical Interfaces	Not selected for migration Routes (Static Routes, ECMP)	Not selected for migration Site-to-Site VPN Tunnels
Not selected for migration Remote Access VPN (Connection Profiles)				

Push Configuration

FMT – 検証に成功しました – 構成をFMCにプッシュします

35. 最後に、Proceedボタンをクリックします。

The Step of final push to target FMC/FTD is subjected to zero, limited or many push errors that largely depend on the success or failure of API execution between migration tool and firewall management center.



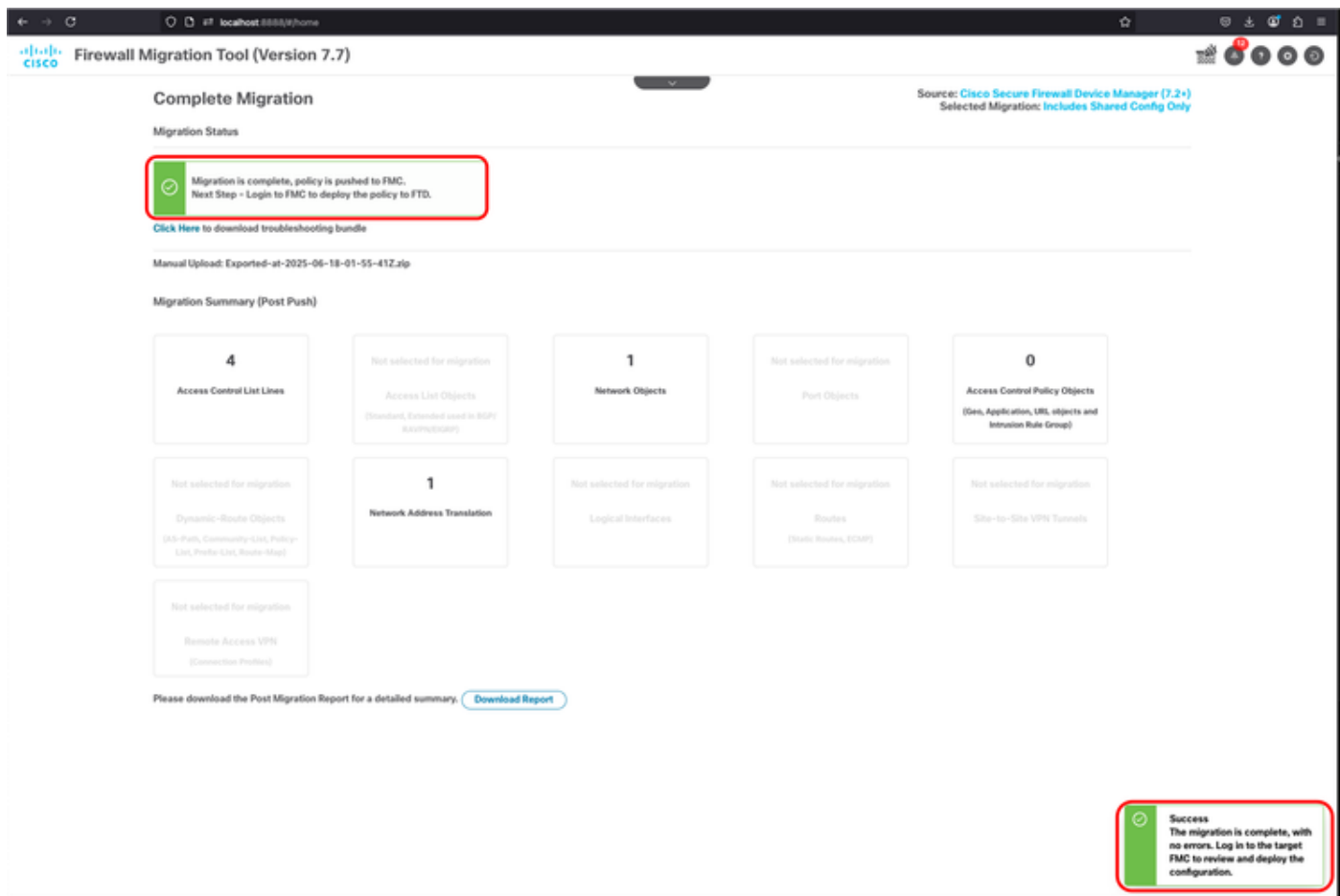
Click on Proceed to continue.

Proceed

Recommendation: Please review the migration fallout report during the course of final push stage to understand firewall configurations that will not be migrated in addition to review the suggested actions to be taken on target FMC for "Abort Migration".

FMT – 構成プッシュの続行

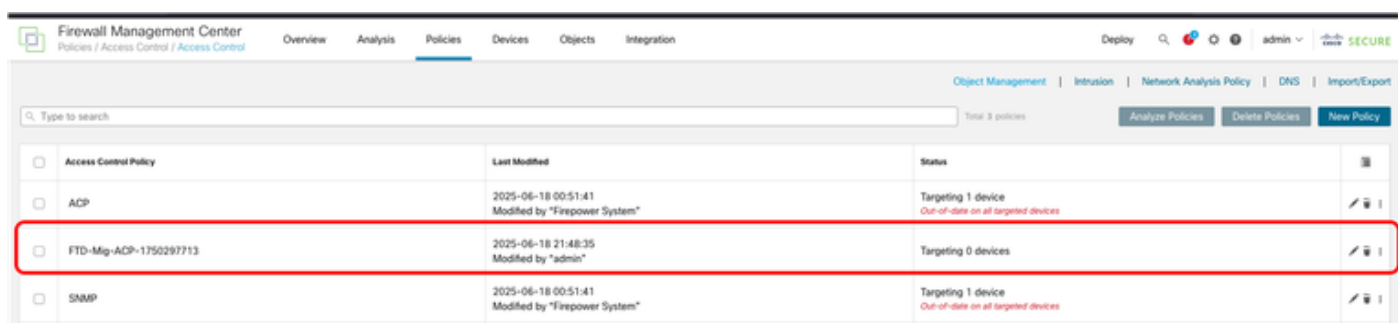
36. すべてが期待どおりに進んだ場合は、「Migration succeeded」通知が表示されます。FMTから、FMCにログインして、移行したポリシーをFTDに展開するように求められます。



FMT:Migration Succeeded通知

FMCの検証

37. FMCにログイン後、ACPおよびNATポリシーがFTD-Migとして表示されます。これで、新しいFTDの導入に進むことができます。



FMC:ACPの移行



FMC:NATポリシーの移行

関連情報

- [FMT - FDMからFMCへの移行ガイド](#)
- [FMTリリースノート](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。